CobiT - Control Objectives

April 1998
2nd Edition

The Control Objectives' Principles

CobiT, as embodied in this latest version of its Control Objectives, reflects the ongoing commitment of ISACA to enhance and maintain the common body of knowledge required to sustain the information systems audit and control profession. Whereas the CobiT Framework focused on high-level controls for each process, Control Objectives focuses on specific, detailed control objectives associated with each IT process. For each of the 34 IT processes of the Framework, there are from three to 30 detailed control objectives. Control Objectives aligns the overall Framework with detailed control objectives from 36 primary sources comprising the de facto and de jure international standards and regulations relating to IT. It contains statements of the desired results or purposes to be achieved by implementing specific control procedures within an IT activity and, thereby, provides a clear policy and good practice for IT control throughout the industry, worldwide.

Control Objectives is directed to the management and staff of the information services, controls, and audit functions - and, most importantly, to the business process owners. Control Objectives provides a working, desktop document for these individuals. Precise and clear definitions of a minimum set of controls to ensure effectiveness, efficiency, and economy of resource utilization are identified. For each process, detailed control objectives are identified as the minimum controls needed to be in place - those controls that will be assessed for sufficiency by the controls professional. There are 302 detailed control objectives that provide an overview of the domain/process/control objective relationships. Control Objectives allows the translation of concepts presented in the Framework into specific controls applicable for each IT process.

Summary Table

The following chart provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives, as well as an indication of which IT resources are applicable.

Planning & Organization (PO)

PO 1.0 Define a Strategic IT Plan

1.1 IT as Part of the organization’s Long- and Short-Range Plan
1.2 IT Long-Range Plan
1.3 IT Long-Range Planning - Approach and Structure
1.4 IT Long-Range Plan Changes
1.5 Short-Range Planning for the Information Services Function
1.6 Assessment of Existing Systems

PO 2.0 Define the Information Architecture

2.1 Information Architecture Model
2.2 Corporate Data Dictionary and Data Syntax Rules
2.3 Data Classification Scheme

2.4 Security Levels

PO 3.0 Determine the Technological Direction

3.1 Technological Infrastructure Planning
3.2 Monitor Future Trends and Regulations
3.3 Technological Infrastructure Contingency
3.4 Hardware and Software Acquisition Plans
3.5 Technology Standards

PO 4.0 Define the IT Organization and Relationships

4.1 The Information Services Function Planning or Steering Committee
4.2 Organizational Placement of Information Services Function
4.3 Review of Organizational Achievements
4.4 Roles and Responsibilities
4.5 Responsibility for Quality Assurance
4.6 Responsibility for Logical and Physical Security
4.7 Ownership and Custodianship
4.8 Data and System Ownership
4.9 Supervision
4.10 Segregation of Duties
4.11 IT Staffing
4.12 Job or Position Descriptions for Information Services Function Staff
4.13 Key IT Personnel
4.14 Contracted Staff Procedures
4.15 Relationships

PO 5.0 Manage the IT Investment

5.1 Annual Information Services Function Operating Budget
5.2 Cost and Benefit Monitoring
5.3 Cost and Benefit Justification

PO 6.0 Communicate Management Aims and Direction

6.1 Positive Information Control Environment
6.2 Management's Responsibility for Policies
6.3 Communication of Organization Policies
6.4 Policy Implementation Resources
6.5 Maintenance of Policies
6.6 Compliance with Polices, Procedures and Standards
6.7 Quality Commitment
6.8 Security and Internal Control Framework Policy
6.9 Intellectual Property Rights
6.10 Issue Specific Policies
6.11 Communication of IT Security Awareness

PO 7.0 Manage Human Resources

7.1 Personnel Recruitment and Promotion
7.2 Personnel Qualifications

7.3 Personnel Training
7.4 Cross-Training or Staff Back-up
7.5 Personnel Clearance Procedures
7.6 Employee Job Performance Evaluation
7.7 Job Change and Termination

PO 8.0 Ensure Compliance with External Requirements

8.1 External Requirements Review
8.2 Practices and Procedures for Complying with External Requirements
8.3 Safety and Ergonomic Compliance
8.4 Privacy, Intellectual Property and Data Flow
8.5 Electronic Commerce
8.6 Compliance with Insurance Contracts

PO 9.0 Assess Risks

9.1 Business Risk Assessment
9.2 Risk Assessment Approach
9.3 Risk Identification
9.4 Risk Measurement
9.5 Risk Action Plan
9.6 Risk Acceptance

PO 10.0 Manage Projects

10.1 Project Management Framework
10.2 User Department Participation in Project Initiation
10.3 Project Team Membership and Responsibilities
10.4 Project Definition
10.5 Project Approval
10.6 Project Phase Approval
10.7 Project Master Plan
10.8 System Quality Assurance Plan
10.9 Planning of Assurance Methods
10.10 Formal Project Risk Management
10.11 Test Plan
10.12 Training Plan
10.13 Post-Implementation Review Plan

PO 11.0 Manage Quality

11.1 General Quality Plan
11.2 Quality Assurance Approach
11.3 Quality Assurance Planning
11.4 Quality Assurance Review of Adherence to the Information Services Function's Standards and Procedures
11.5 System Development Life Cycle Methodology
11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology

11.7 Updating the System Development Life Cycle Methodology
11.8 Coordination and Communication
11.9 Acquisition and Maintenance Framework for the Technology Infrastructure
11.10 Third-Party Implementor Relationships
11.11 Program Documentation Standards
11.12 Program Testing Standards
11.13 System Testing Standards
11.14 Parallel/Pilot Testing
11.15 System Testing Documentation
11.16 Quality Assurance Evaluation of Adherence to Development Standards
11.17 Quality Assurance Review of the Achievement of the Information Services Function's Objectives
11.18 Quality Metrics
11.19 Reports of Quality Assurance Reviews

Acquisition & Implementation (AI)

AI 1.0 Identify Solutions

1.1 Definition of Information Requirements
1.2 Formulation of Alternative Courses of Action
1.3 Formulation of Acquisition Strategy
1.4 Third-Party Service Requirements
1.5 Technological Feasibility Study
1.6 Economic Feasibility Study
1.7 Information Architecture
1.8 Risk Analysis Report
1.9 Cost-Effective Security Controls
1.10 Audit Trails Design
1.11 Ergonomics
1.12 Selection of System Software
1.13 Procurement Control
1.14 Software Product Acquisition
1.15 Third-Party Software Maintenance
1.16 Contract Application Programming
1.17 Acceptance of Facilities
1.18 Acceptance of Technology

AI 2.0 Acquire and Maintain Application Software

2.1 Design Methods
2.2 Major Changes to Existing Systems
2.3 Design Approval
2.4 File Requirements Definition and Documentation
2.5 Program Specifications
2.6 Source Data Collection Design
2.7 Input Requirements Definition and Documentation

2.8 Definition of Interfaces

2.9 User-Machine Interface

2.10 Processing Requirements Definition and Documentation

2.11 Output Requirements Definition and Documentation

2.12 Controllability

2.13 Availability as Key Design Factor

2.14 IT Integrity Provisions in Application Program Software

2.15 Application Software Testing

2.16 User Reference and Support Materials

2.17 Re-Assessment of System Design

AI 3.0 Acquire and Maintain Technology Architecture

3.1 Assessment of New Hardware and Software

3.2 Preventative Maintenance for Hardware

3.3 System Software Security

3.4 System Software Installation

3.5 System Software Maintenance

3.6 System Software Change Controls

AI 4.0 Develop and Maintain IT Procedures

4.1 Future Operational Requirements and Service Levels

4.2 User Procedures Manual

4.3 Operations Manual

4.4 Training Materials

AI 5.0 Install and Accredit Systems

5.1 Training

5.2 Application Software Performance Sizing

5.3 Conversion

5.4 Testing of Changes

5.5 Parallel/Pilot Testing Criteria and Performance

5.6 Final Acceptance Test

5.7 Security Testing and Accreditation

5.8 Operational Test

5.9 Promotion to Production

5.10 Evaluation of Meeting User Requirements

5.11 Management's Post-Implementation Review

AI 6.0 Manage Changes

6.1 Change Request Initiation and Control

6.2 Impact Assessment

6.3 Control of Changes

6.4 Documentation and Procedures

6.5 Authorized Maintenance

6.6 Software Release Policy

6.7 Distribution of Software

Delivery & Support (DS)

DS 1.0 Define Service Levels

1.1 Service Level Agreement Framework
1.2 Aspects of Service Level Agreements
1.3 Performance Procedures
1.4 Monitoring and Reporting
1.5 Review of Service Level Agreements and Contracts
1.6 Chargeable Items
1.7 Service Improvement Program

DS 2.0 Manage Third-Party Services

2.1 Supplier Interfaces
2.2 Owner Relationships
2.3 Third-Party Contracts
2.4 Third-Party Qualifications
2.5 Outsourcing Contracts
2.6 Continuity of Services
2.7 Security Relationships
2.8 Monitoring

DS 3.0 Manage Performance and Capacity

3.1 Availability and Performance Requirements
3.2 Availability Plan
3.3 Monitoring and Reporting
3.4 Modeling Tools
3.5 Proactive Performance Management
3.6 Workload Forecasting
3.7 Capacity Management of Resources
3.8 Resources Availability
3.9 Resources Schedule

DS 4.0 Ensure Continuous Service

4.1 IT Continuity Framework
4.2 IT Continuity Plan Strategy and Philosophy
4.3 IT Continuity Plan Contents
4.4 Minimizing IT Continuity Requirements
4.5 Maintaining the IT Continuity Plan
4.6 Testing the IT Continuity Plan
4.7 IT Continuity Plan Training
4.8 IT Continuity Plan Distribution
4.9 User Department Alternative Processing Back-up Procedures
4.10 Critical IT Resources
4.11 Back-up Site and Hardware

4.12 Wrap-up Procedures

DS 5.0 Ensure Systems Security

5.1 Manage Security Measures
5.2 Identification, Authentication and Access
5.3 Security of Online Access to Data
5.4 User Account Management
5.5 Management Review of User Accounts
5.6 User Control of User Accounts
5.7 Security Surveillance
5.8 Data Classification
5.9 Central Identification and Access Rights Management
5.10 Violation and Security Activity Reports
5.11 Incident Handling
5.12 Re-Accreditation
5.13 Counterparty Trust
5.14 Transaction Authorization
5.15 Non-Repudiation
5.16 Trusted Path
5.17 Protection of Security Functions
5.18 Cryptographic Key Management
5.19 Malicious Software Prevention, Detection and Correction
5.20 Firewall Architectures and Connections with Public Networks
5.21 Protection of Electronic Value

DS 6.0 Identify and Attribute Costs

6.1 Chargeable Items
6.2 Costing Procedures
6.3 User Billing and Chargeback Procedures

DS 7.0 Educate and Train Users

7.1 Identification of Training Needs
7.2 Training Organization
7.3 Security Principles and Awareness Training

DS 8.0 Assist and Advise IT Customers

8.1 Help Desk
8.2 Registration of Customer Queries
8.3 Customer Query Escalation
8.4 Monitoring of Clearance
8.5 Trend Analysis and Reporting

DS 9.0 Manage the Configuration

9.1 Configuration Recording
9.2 Configuration Baseline
9.3 Status Accounting

9.4 Configuration Control
9.5 Unauthorized Software
9.6 Software Storage

DS 10.0 Manage Problems and Incidents

10.1 Problem Management System
10.2 Problem Escalation
10.3 Problem Tracking and Audit Trail

DS 11.0 Manage Data

11.1 Data Preparation Procedures
11.2 Source Document Authorization Procedures
11.3 Source Document Data Collection
11.4 Source Document Error Handling
11.5 Source Document Retention
11.6 Data Input Authorization Procedures
11.7 Accuracy, Completeness and Authorization Checks
11.8 Data Input Error Handling
11.9 Data Processing Integrity
11.10 Data Processing Validation and Editing
11.11 Data Processing Error Handling
11.12 Output Handling and Retention
11.13 Output Distribution
11.14 Output Balancing and Reconciliation
11.15 Output Review and Error Handling
11.16 Security Provision for Output Reports
11.17 Protection of Sensitive Information during Transmission and Transport
11.18 Protection of Disposed Sensitive Information
11.19 Storage Management
11.20 Retention Periods and Storage Terms
11.21 Media Library Management System
11.22 Media Library Management Responsibilities
11.23 Back-up and Restoration
11.24 Back-up Jobs
11.25 Back-up Storage
11.26 Archiving
11.27 Protection of Sensitive Messages
11.28 Authentication and Integrity
11.29 Electronic Transaction Integrity
11.30 Continued Integrity of Stored Data

DS 12.0 Manage Facilities

12.1 Physical Security
12.2 Low Profile of the IT Site
12.3 Visitor Escort
12.4 Personnel Health and Safety

12.5 Protection against Environmental Factors
12.6 Uninterruptable Power Supply

DS 13.0 Manage Operations

13.1 Processing Operations Procedures and Instructions Manual
13.2 Startup Process and Other Operations Documentation
13.3 Job Scheduling
13.4 Departures from Standard Job Schedules
13.5 Processing Continuity
13.6 Operations Logs
13.7 Remote Operations

Monitoring (M)

M 1.0 Monitor the Processes

1.1 Collecting Monitoring Data
1.2 Assessing Performance
1.3 Assessing Customer Satisfaction
1.4 Management Reporting

M 2.0 Assess Internal Control Adequacy

2.1 Internal Control Monitoring
2.2 Timely Operation of Internal Controls
2.3 Internal Control Level Reporting
2.4 Operational Security and Internal Control Assurance

M 3.0 Obtain Independent Assurance

3.1 Independent Security and Control Certification/Accreditation of IT Services
3.2 Independent Security and Control Certification/Accreditation of Third-Party Service Providers
3.3 Independent Effectiveness Evaluation of IT Services
3.4 Independent Effectiveness Evaluation of Third-Party Service Providers
3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments
3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
3.7 Competence of Independent Assurance Function
3.8 Proactive Audit Involvement

M 4.0 Provide for Independent Audit

4.1 Audit Charter
4.2 Independence
4.3 Professional Ethics and Standards

4.4 Competence
4.5 Planning
4.6 Performance of Audit Work
4.7 Reporting
4.8 Follow-up Activities

The Control Objectives

On the following pages are itemized detailed control objectives for each of the 34 processes within an information technology function.

Planning and Organization (PO)

PO 1.0 - Define a Strategic Information Technology Plan

1.1 Information Technology as Part of the organization’s Long- and Short-Range Plan

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organization’s mission and goals. In this respect, senior management should ensure that information technology issues as well as opportunities are adequately assessed and reflected in the organization’s long- and short-range plans.

1.2 Information Technology Long-Range Plan

Management of the information services function is responsible for regularly developing information technology long-range plans supporting the achievement of the organization’s overall missions and goals. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

1.3 Information Technology Long-Range Planning - Approach and Structure

Management of the information services function should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan which covers the basic questions of what, who, how, when and why. Aspects which need to be taken into account and adequately addressed during the planning process are the organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the market, planning horizon, business process re-engineering, staffing, in- or out-sourcing, etc. Benefits of the choices made should be clearly identified. The plan itself should also refer to other plans such as the organization quality plan and the information risk management plan.

1.4 Information Technology Long-Range Plan Changes

Management of the information services function should ensure a process is in place to timely and accurately modify the information technology long-range plan to accommodate changes to the organization’s long-range plan and changes in information technology conditions.

1.5 Short-Range Planning for the Information Services Function

Management of the information services function should ensure that the information technology long-range plan is regularly translated into information technology short-range plans. Such short-range plans should ensure that appropriate information services function resources are allocated on a basis consistent with the information technology long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and information technology conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

1.6 Assessment of Existing Systems

Prior to developing or changing the strategic information technology plan, management of the information services function should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses, in order to determine the degree to which the existing systems support the organization's business requirements.

PO 2.0 - Define the Information Architecture

2.1 Information Architecture Model

Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the information services function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the information technology long-range plan.

2.2 Corporate Data Dictionary and Data Syntax Rules

The information services function should ensure the creation and continuous updating of a corporate data dictionary which incorporates the organization's data syntax rules.

2.3 Data Classification Scheme

A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.

2.4 Security Levels

Management should define, implement and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications.

PO 3.0 - Determine Technological Direction

3.1 Technological Infrastructure Planning

The information services function should create and regularly update a technological infrastructure plan which is in accordance with the information technology long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction and migration strategies.

3.2 Monitor Future Trends and Regulations

Continuous monitoring of future trends and regulatory conditions should be ensured by the information services function so that these factors can be taken into consideration during the development and maintenance of the technological infrastructure plan.

3.3 Technological Infrastructure Contingency

The technological infrastructure plan should be assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).

3.4 Hardware and Software Acquisition Plans

Management of the information services function should ensure that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan.

3.5 Technology Standards

Based on the technological infrastructure plan, management should define technology norms in order to foster standardization.

PO 4.0 - Define the Information Technology Organization and Relationships

4.1 The Information Services Function Planning or Steering Committee

The organization’s senior management should appoint a planning or steering committee to oversee the information services function and its activities. Committee membership should include representatives from senior management, user management and the information services function. The committee should meet regularly and report to senior management.

4.2 Organizational Placement of Information Services Function

In placing the information services function in the overall organization structure, senior management should ensure authority, critical mass and independence from user departments to the degree necessary to guarantee effective information technology solutions and sufficient progress in implementing them, and to establish a partnership relation with top management to help increase awareness, understanding and skill in identifying and resolving information technology issues.

4.3 Review of Organizational Achievements

A framework should be in place for reviewing the organizational structure to continuously meet objectives and changing circumstances.

4.4 Roles and Responsibilities

Management should ensure that all personnel in the organization have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organized and undertaken to increase awareness and discipline.

4.5 Responsibility for Quality Assurance

Management should assign the responsibility for the performance of the quality assurance function to staff members of the information services function and ensure that appropriate quality assurance, systems, controls and communications expertise exist in the information services function's quality assurance group. The organizational placement within the information services function, the responsibilities and the size of the quality assurance group should satisfy the requirements of the organization.

4.6 Responsibility for Logical and Physical Security

Management should formally assign the responsibility for assuring both the logical and physical security of the organization’s information assets to an information security manager, reporting to the organization’s senior management. At a minimum, security management responsibility should be established at the organization-wide level to deal with overall security issues in an organization. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.

4.7 Ownership and Custodianship

Management should create a structure for formally appointing the data owners and custodians. Their roles and responsibilities should be clearly defined.

4.8 Data and System Ownership

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

4.9 Supervision

Senior management should implement adequate supervisory practices in the information services organization to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.

4.10 Segregation of Duties

Senior management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between the following functions:

* information systems use;
* data entry;
* computer operation;
* network management;
* system administration;
* systems development and maintenance;
* change management;
* security administration; and
* security audit.

4.11 Information Technology Staffing

Staffing requirements evaluations should be performed regularly to ensure the information services function has a sufficient number of competent information technology staff. Staffing requirements should be evaluated at least annually or upon major changes to the business, operational or information technology environment. Evaluation results should be acted upon promptly to ensure adequate staffing currently and in the future.

4.12 Job or Position Descriptions for Information Services Function Staff

Management should ensure that position descriptions for information services function staff are established and updated regularly. These position descriptions should clearly delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and be suitable for use in performance evaluation.

4.13 Key Information Technology Personnel

Management should define and identify key information technology personnel.

4.14 Contracted Staff Procedures

Management should define and implement relevant procedures for controlling the activities of consultants and other contract personnel by the information services function to assure the protection of the organization's information assets.

4.15 Relationships

Management of the information services function should undertake the necessary actions to establish and maintain an optimal coordination, communication and liaison structure between the information services function and various other interests inside and outside the information services function (i.e., users, suppliers, security officers, risk managers).

PO 5.0 - Manage the Information Technology Investment

5.1 Annual Information Services Function Operating Budget

Senior management should implement a budgeting process to ensure that an annual information services function operating budget is established and approved in line with the organization's long- and short-range plans as well as with the information technology long- and short-range plans. Funding alternatives should be investigated.

5.2 Cost and Benefit Monitoring

Management should establish a cost monitoring process comparing actuals to budgets. Moreover, the possible benefits derived from the information technology activities should be determined and reported. For cost monitoring, the source of the actual figures should be based upon the organization's accounting system and that system should routinely record, process and report the costs associated with the activities of the information services function. For benefit monitoring, high-level performance indicators should be defined, regularly reported and reviewed for adequacy.

5.3 Cost and Benefit Justification

A management control should be in place to guarantee that the delivery of services by the information services function is cost justified and in line with the industry. The benefits derived from the information technology activities should similarly be analyzed.

PO 6.0 - Communicate Management Aims and Direction

6.1 Positive Information Control Environment

Management should create a framework and an awareness program fostering a positive control environment throughout the entire organization by addressing aspects such as: integrity, ethical values and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors. Specific attention is to be given to information technology aspects.

6.2 Management's Responsibility for Policies

Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives. Regular reviews of policies for appropriateness should be carried out. The complexity of the written policies and procedures should always be commensurate with the organization size and management style.

6.3 Communication of Organization Policies

Management should ensure that organizational policies are communicated to and understood by all levels in the organization.

6.4 Policy Implementation Resources

After communication, appropriate resources should be earmarked by management for the implementation of its policies. Management should also monitor the timeliness of the policy implementation.

6.5 Maintenance of Policies

Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives and procedures.

6.6 Compliance with Polices, Procedures and Standards

Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed. Compliance procedures for ethical, security, and internal control standards should be set by top management and promoted by example.

6.7 Quality Commitment

Management of the information services function should define, document and maintain a quality philosophy, policies and objectives which are consistent with the corporate philosophies and policies in this regard. The quality philosophy, policies and objectives should be understood, implemented and maintained at all levels of the information services function.

6.8 Security and Internal Control Framework Policy

Senior management should assume full responsibility for developing and maintaining a framework policy which establishes the organization's overall approach to security and internal control. The policy should comply with overall business objectives and be aimed at minimization of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration. Measures should be based on cost-benefit analyses and should be prioritized. In addition, senior management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organization, the definition and assignment of responsibilities for implementation at all levels, and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies.

6.9 Intellectual Property Rights

Management should provide and implement a written policy on intellectual property rights covering in-house as well as contract-developed software.

6.10 Issue Specific Policies

Measures should be put in place to ensure that issue-specific policies are established to document management decisions in addressing particular activities, applications, systems or technologies.

6.11 Communication of IT Security Awareness

An information technology security awareness program should communicate the information technology security policy to each information technology user and assure a complete understanding of the importance of information technology security. It should convey the message that information technology security is to the benefit of the organization, all its employees, and that everybody is responsible for it. The information technology security awareness program should be supported by, and represent the view of senior management.

PO 7.0 - Manage Human Resources

7.1 Personnel Recruitment and Promotion

Management should implement and regularly assess the needed processes to ensure that personnel recruiting and promotion practices are based on objective criteria and consider education, experience and responsibility. These processes should be in line with the overall organization's policies and procedures in this regard.

7.2 Personnel Qualifications

Management of the information services function should regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training and/or experience, as required. Management should encourage personnel to obtain membership in professional organizations.

7.3 Personnel Training

Management should ensure that employees are provided with orientation upon hiring and with on-going training to maintain their knowledge, skills, abilities and security awareness to the level required to perform effectively. Education and training programs conducted to effectively raise the technical and management skill levels of personnel should be reviewed regularly.

7.4 Cross-Training or Staff Back-up

Management should provide for sufficient cross-training or back-up of identified key personnel to address unavailabilities. Personnel in sensitive positions should be required to take uninterrupted holidays of sufficient length to exercise the organization's ability to cope with unavailabilities and to detect fraudulent activity.

7.5 Personnel Clearance Procedures

Management of the information services function should ensure that their personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. An employee who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

7.6 Employee Job Performance Evaluation

Management should implement an employee performance evaluation process and make sure that the evaluation is performed against established standards and specific job responsibilities on a regular basis. Employees should receive counseling on performance or conduct whenever appropriate.

7.7 Job Change and Termination

Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

PO 8.0 - Ensure Compliance with External Requirements

8.1 External Requirements Review

The organization should establish and maintain procedures for external requirements review and for the coordination of these activities. Continuous research should determine the applicable external requirements for the organization. Legal, government or other external requirements related to information technology practices and controls should be reviewed. Management should also assess the impact of any external relationships on the organization’s overall information needs including determination of the extent to which information services function strategies need to conform with or support the requirements of any related third-parties.

8.2 Practices and Procedures for Complying with External Requirements

Organizational practices should ensure that appropriate corrective actions are taken on a timely basis to guarantee compliance with external requirements. In addition, adequate procedures assuring continuous compliance should be established and maintained. In this regard, management should seek legal advice if required.

8.3 Safety and Ergonomic Compliance

Management should ensure compliance with safety and ergonomic standards in the working environment of information services function users and personnel.

8.4 Privacy, Intellectual Property and Data Flow

Management should ensure compliance with privacy, intellectual property, trans-border data flow and cryptographic regulations applicable to the information technology practices of the organization.

8.5 Electronic Commerce

Management should ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage. When trading on the Internet, management should enforce adequate controls to ensure compliance with local laws and customs on a worldwide basis.

8.6 Compliance with Insurance Contracts

Management should ensure that insurance contract requirements are properly identified and continuously met.

PO 9.0 - Assess Risks

9.1 Business Risk Assessment

Management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the global level and system specific levels (for new projects as well as on a recurring basis) and should ensure regular updates of the risk assessment information with results of audits, inspections and identified incidents.

9.2 Risk Assessment Approach

Management should establish a general risk assessment approach which defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.

9.3 Risk Identification

The risk assessment approach should focus on the examination of the essential elements of risk such as assets, threats, vulnerabilities, safeguards, consequences and likelihood of threat.

9.4 Risk Measurement

The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organization should also be assessed.

9.5 Risk Action Plan

The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis.

9.6 Risk Acceptance

The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organizational policy, uncertainty incorporated in the risk assessment approach itself and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage.

PO 10.0 - Manage Projects

10.1 Project Management Framework

Management should establish a general project management framework which defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points and approvals.

10.2 User Department Participation in Project Initiation

The organization’s project management framework should provide for participation by the affected user department management in the definition and authorization of a development, implementation or modification project.

10.3 Project Team Membership and Responsibilities

The organization’s project management framework should specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members.

10.4 Project Definition

The organization’s project management framework should provide for the creation of a clear written statement defining the nature and scope of every implementation project before work on the project begins.

10.5 Project Approval

The organization’s project management framework should ensure that for each proposed project, the organization’s senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project.

10.6 Project Phase Approval

The organization’s project management framework should provide for designated managers of the user and information services functions to approve the work accomplished in each phase of the cycle before work on the next phase begins.

10.7 Project Master Plan

Management should ensure that for each approved project a project master plan is created which is adequate for maintaining control over the project throughout its life and which includes a method of monitoring the time and costs incurred throughout the life of the project.

10.8 System Quality Assurance Plan

Management should ensure that the implementation of a new or modified system includes the preparation of a quality plan which is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.

10.9 Planning of Assurance Methods

Assurance tasks are to be identified during the planning phase of the project management framework. Assurance tasks should support the accreditation of new or modified systems and should assure that internal controls and security features meet the related requirements.

10.10 Formal Project Risk Management

Management should implement a formal project risk management program for eliminating or minimizing risks associated with individual projects (i.e., identifying and controlling the areas or events that have the potential to cause unwanted change).

10.11 Test Plan

The organization’s project management framework should require that a test plan be created for every development, implementation and modification project.

10.12 Training Plan

The organization’s project management framework should require that a training plan be created for every development, implementation and modification project.

10.13 Post-Implementation Review Plan

The organization’s project management framework should provide, as an integral part of the project team's activities, for the development of a plan for a post-implementation review of every new or modified information system to ascertain whether the project has delivered the planned benefits.

PO 11.0 - Manage Quality

11.1 General Quality Plan

Senior management should develop and regularly maintain an overall quality plan based on the organizational and information technology long-range plans. The plan should promote the continuous improvement philosophy and answer the basic questions of what, who and how.

11.2 Quality Assurance Approach

Management should establish a standard approach regarding quality assurance which covers both general and project specific quality assurance activities. The approach should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.)

to be performed to achieve the objectives of the general quality plan. It should also require specific quality assurance reviews.

11.3 Quality Assurance Planning

Management should implement a quality assurance planning process to determine the scope and timing of the quality assurance activities.

11.4 The Quality Assurance Review of Adherence to the Information Services Function's Standards and Procedures

Management should ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to the information services function's standards and procedures.

11.5 System Development Life Cycle Methodology

The organization’s senior management should define and implement information systems standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerized information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.

11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology

In the event of major changes to existing technology, management should ensure that a system development life cycle methodology is observed, as in the case of the acquisition of new technology.

11.7 Updating of the System Development Life Cycle Methodology

Senior management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.

11.8 Coordination and Communication

Management should establish a process for ensuring close coordination and communication between customers of the information services function and system implementors. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality information technology solutions which meet the business demands. Management should promote an organization which is characterized by close cooperation and communication throughout the system development life cycle.

11.9 Acquisition and Maintenance Framework for the Technology Infrastructure

A general framework should be in place regarding the acquisition and maintenance of the technology infrastructure. The different steps to be followed regarding the technology infrastructure (such as acquiring; programming, documenting, and testing; parameter setting; maintaining and applying fixes) should be governed by, and in line with, the acquisition and maintenance framework for the technology infrastructure.

11.10 Third-Party Implementor Relationships

Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards and procedures.

11.11 Program Documentation Standards

The organization's system development life cycle methodology should incorporate standards for program documentation which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

11.12 Program Testing Standards

The organization's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.

11.13 System Testing Standards

The organization's system development life cycle methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.

11.14 Parallel/Pilot Testing

The organization's system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.

11.15 System Testing Documentation

The organization's system development life cycle methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.

11.16 Quality Assurance Evaluation of Adherence to Development Standards

The organization's quality assurance approach should require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology.

11.17 The Quality Assurance Review of the Achievement of the Information Services Function's Objectives

The quality assurance approach should include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function.

11.18 Quality Metrics

Management should define and use metrics to measure the results of activities, thus assessing whether quality goals have been achieved.

11.19 Reports of Quality Assurance Reviews

Reports of quality assurance reviews should be prepared and submitted to management of user departments and the information services function.

Acquisition and Implementation (AI)

AI 1.0 - Identify Solutions

1.1 Definition of Information Requirements

The organization’s system development life cycle methodology should provide that the business requirements satisfied by the existing system and to be satisfied by the proposed new or modified system (software, data and infrastructure) be clearly defined before a development, implementation or modification project is approved. The system development life cycle methodology should require that the solution's functional and operational requirements be specified including performance, safety, reliability, compatibility, security and legislation.

1.2 Formulation of Alternative Courses of Action

The organization’s system development life cycle methodology should provide for the analysis of the alternative courses of action that will satisfy the business requirements established for a proposed new or modified system.

1.3 Formulation of Acquisition Strategy

The organization’s system development life cycle methodology should provide for a software acquisition strategy plan defining whether the software will be acquired off-the-shelf, developed internally, through contract or by enhancing the existing software, or a combination of all these.

1.4 Third-Party Service Requirements

The organization’s system development life cycle methodology should provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.

1.5 Technological Feasibility Study

The organization’s system development life cycle methodology should provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.

1.6 Economic Feasibility Study

The organization's system development life cycle methodology should provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.

1.7 Information Architecture

Management should ensure that attention is paid to the enterprise data model while solutions are being identified and analyzed for feasibility.

1.8 Risk Analysis Report

The organization's system development life cycle methodology should provide, in each proposed information system development, implementation or modification project, for an analysis and documentation of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk. This should be realized in line with the overall risk assessment framework.

1.9 Cost-Effective Security Controls

Management should ensure that the costs and benefits of security are carefully examined in monetary and non-monetary terms to guarantee that the costs of controls do not exceed benefits. The decision requires formal management sign-off.

1.10 Audit Trails Design

The organization's system development life cycle methodology should require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g., user ID's) against discovery and misuse.

1.11 Ergonomics

Management should ensure that the information system development, implementation and change projects undertaken by the information services function pay attention to ergonomic issues associated with the introduction of automated solutions.

1.12 Selection of System Software

Management should ensure that a standard procedure is adhered to by the information services function to identify all potential system software programs that will satisfy its operational requirements.

1.13 Procurement Control

Management should develop and implement a central procurement approach describing a common set of procedures and standards to be followed in the procurement of information technology related hardware, software and services. Products should be reviewed and tested prior to their use and the financial settlement.

1.14 Software Product Acquisition

Software product acquisition should follow the organization’s procurement policies.

1.15 Third-Party Software Maintenance

Management should require that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights. Consideration should be given to the support of the product in any maintenance agreement related to the delivered product.

1.16 Contract Application Programming

The organization’s system development life cycle methodology should provide that the procurement of contract programming services be justified with a written request for services from a designated member of the information services function. The contract should stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance. In addition, it should require that the end products of completed contract programming services be tested and reviewed according to the related standards by the information services function's quality assurance group and other concerned parties (such as users, project managers, etc.) before payment for the work and approval of the end product. Testing to be included in contract specifications should consist of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure.

1.17 Acceptance of Facilities

Management should ensure that an acceptance plan for facilities to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests should be performed to guarantee that the accommodation and environment meet the requirements specified in the contract.

1.18 Acceptance of Technology

Management should ensure that an acceptance plan for specific technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests provided for in the plan should include inspection, functionality tests and workload trials.

AI 2.0 - Acquire and Maintain Application Software

2.1 Design Methods

The organization’s system development life cycle methodology should provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.

2.2 Major Changes to Existing Systems

Management should ensure, that in the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.

2.3 Design Approval

The organization's system development life cycle methodology should require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organization's senior management, when appropriate.

2.4 File Requirements Definition and Documentation

The organization's system development life cycle methodology should provide that an appropriate procedure be applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the data dictionary rules are respected.

2.5 Program Specifications

The organization's system development life cycle methodology should require that detailed written program specifications be prepared for each information system development or modification project. The methodology should further ensure that program specifications agree with system design specifications.

2.6 Source Data Collection Design

The organization's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.

2.7 Input Requirements Definition and Documentation

The organization's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.

2.8 Definition of Interfaces

The organization's system development life cycle methodology should provide that all external and internal interfaces are properly specified, designed and documented.

2.9 User-Machine Interface

The organization's system development life cycle methodology should provide for the development of an interface between the user and machine which is easy to use and self-documenting (by means of online help functions).

2.10 Processing Requirements Definition and Documentation

The organization's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project.

2.11 Output Requirements Definition and Documentation

The organization’s system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project.

2.12 Controllability

The organization’s system development life cycle methodology should require that adequate mechanisms for assuring the internal control and security requirements be specified for each information system development or modification project. The methodology should further ensure that information systems are designed to include application controls which guarantee the accuracy, completeness, timeliness and authorization of inputs, processing and outputs. Sensitivity assessment should be performed during initiation of system development or modification. The basic security and internal control aspects of a system to be developed or modified should be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible.

2.13 Availability as a Key Design Factor

The organization’s system development life cycle methodology should provide that availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability should be analyzed and, if necessary, increased through maintainability and reliability improvements.

2.14 Information Technology Integrity Provisions in Application Program Software

The organization should establish procedures to assure, where applicable, that application programs contain provisions which routinely verify the tasks performed by the software to help assure data integrity, and which provide in the restoration of the integrity through rollback or other means.

2.15 Application Software Testing

Unit testing, application testing, integration testing, system testing, and load and stress testing should be performed according to the project test plan and established testing standards before it is approved by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

2.16 User Reference and Support Materials

The organization’s system development life cycle methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every information system development or modification project.

2.17 Re-Assessment of System Design

The organization’s system development life cycle methodology should ensure that the system design is re-assessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.

AI 3.0 - Acquire and Maintain Technology Architecture

3.1 Assessment of New Hardware and Software

Procedures should be in place to assess new hardware and software for any impact on the performance of the overall system.

3.2 Preventative Maintenance for Hardware

Management of the information services function should schedule routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.

3.3 System Software Security

Management of the information services function should ensure that the set-up of system software to be installed does not jeopardize the security of the data and programs being stored on the system. Attention should be paid to set-up and maintenance of system software parameters.

3.4 System Software Installation

Procedures should be implemented to ensure that system software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing should be performed before use in the production environment is authorized.

3.5 System Software Maintenance

Procedures should be implemented to ensure that system software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.

3.6 System Software Change Controls

Procedures should be implemented to ensure that system software changes are controlled in line with the organization’s change management procedures.

AI 4.0 - Develop and Maintain Information Technology Procedures

4.1 Future Operational Requirements and Service Levels

The organization’s system development life cycle methodology should ensure the timely definition of future operational requirements and service levels.

4.2 User Procedures Manuals

The organization’s system development life cycle methodology should provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.

4.3 Operations Manual

The organization’s system development life cycle methodology should provide that an adequate operations manual be prepared and kept up-to-date as part of every information system development, implementation or modification project.

4.4 Training Materials

The organization’s system development life cycle methodology should assure that adequate training materials are developed as part of every information system development, implementation or modification project. These materials should be focused on the system's use in daily practice.

AI 5.0 - Install and Accredit Systems

5.1 Training

Staff of the affected user departments and the operations group of the information services function should be trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.

5.2 Application Software Performance Sizing

Application software performance sizing (optimization) should be established as an integral part of the organization’s system development life cycle methodology to forecast the resources required for operating new and significantly changed software.

5.3 Conversion

The organization’s system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan.

5.4 Testing of Changes

Management should ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans should also be developed. Acceptance testing should be carried out in an environment representative of the future operational environment (e.g., similar security, internal controls, workloads, etc.)

5.5 Parallel/Pilot Testing Criteria and Performance

Procedures should be in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance.

5.6 Final Acceptance Test

Procedures should provide, as part of the final acceptance or quality assurance testing of new or modified information systems, for a formal evaluation and approval of the test results by management of the affected user department(s) and the information services function. The tests should cover all components of the information system (e.g., application software, facilities, technology, user procedures).

5.7 Security Testing and Accreditation

Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk.

5.8 Operational Test

Management should ensure that before moving the system into operation, the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment.

5.9 Promotion to Production

Management should define and implement formal procedures to control the handover of the system from development to testing to operations. The respective environments should be segregated and properly protected.

5.10 Evaluation of Meeting User Requirements

The organization’s system development life cycle methodology should require that a post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) be conducted to assess whether the users' needs are being achieved by the system.

5.11 Management's Post-Implementation Review

The organization’s system development life cycle methodology should require that a post-implementation review of an operational information system assess and report on whether the system delivered the benefits envisioned in the most cost effective manner.

AI 6.0 - Manage Changes

6.1 Change Request Initiation and Control

Management should ensure that all requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.

6.2 Impact Assessment

A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

6.3 Control of Changes

Management should ensure that change management, and software control and distribution are properly integrated with a comprehensive configuration management system.

6.4 Documentation and Procedures

The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

6.5 Authorized Maintenance

Management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.

6.6 Software Release Policy

Management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.

6.7 Distribution of Software

Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.

Delivery and Support (DS)

DS 1.0 - Define Service Levels

1.1 Service Level Agreement Framework

Senior management should define a framework wherein it promotes the definition of formal service level agreements and defines the minimal contents: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures. Users and the information services function should have a written agreement which describes the service level in qualitative and quantitative terms. The agreement defines the responsibilities of both parties. The information services function must offer the agreed quality and quantity of service and the users must constrain the demands they place upon the service within the agreed limits.

1.2 Aspects of Service Level Agreements

Explicit agreement should be reached on the aspects that a service level agreement should have. The service level agreement should cover at least the following aspects: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures.

1.3 Performance Procedures

Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.

1.4 Monitoring and Reporting

Information services function management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analyzed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.

1.5 Review of Service Level Agreements and Contracts

Management should implement a regular review process for service level agreements and underpinning contracts with third-party service providers.

1.6 Chargeable Items

Provisions for chargeable items should be included in the service level agreements to make trade-offs possible on service levels versus costs.

1.7 Service Improvement Program

Management should implement a process to ensure that users and service level managers regularly agree on a service improvement program for pursuing cost-justified improvements to the service level.

DS 2.0 - Manage Third-Party Services

2.1 Supplier Interfaces

Management should ensure that all third-party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented.

2.2 Owner Relationships

The customer organization management should appoint a relationship owner who is responsible for ensuring the quality of the relationships with third-parties.

2.3 Third-Party Contracts

Management should define specific procedures to ensure that for each relationship with a third-party service provider a formal contract is defined and agreed upon.

2.4 Third-Party Qualifications

Management should ensure that, before selection, potential third-parties are properly qualified through an assessment of their capability to deliver the required service (due diligence).

2.5 Outsourcing Contracts

Specific organizational procedures should be defined to ensure that the contract between the facilities management provider and the organization is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.

2.6 Continuity of Services

With respect to ensuring continuity of services, management should consider business risk related to the third-party in terms of legal uncertainties and the going concern concept, and negotiate escrow contracts where appropriate.

2.7 Security Relationships

With regard to relationships with third-party service providers, management should ensure that security agreements (e.g., non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.

2.8 Monitoring

A continuous process for monitoring of the service delivery of the third-party should be set up by management to ensure the adherence to the contract agreements.

DS 3.0 - Manage Performance and Capacity

3.1 Availability and Performance Requirements

The management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.

3.2 Availability Plan

Management should ensure the establishment of an availability plan to achieve, monitor and control the availability of information services.

3.3 Monitoring and Reporting

Management should implement a process to ensure that the performance of information technology resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.

3.4 Modeling Tools

Management should ensure that appropriate modeling tools are used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels. Modeling tools should be used to assist with the prediction of capacity, configuration reliability, performance and availability requirements. In depth technical investigations should be conducted on systems hardware and should include forecasts concerning future technologies.

3.5 Proactive Performance Management

The performance management process should include forecasting capability to enable problems to be corrected before they affect system performance. Analysis should be conducted on system failures and irregularities pertaining to frequency, degree of impact and amount of damage.

3.6 Workload Forecasting

Controls are to be in place to ensure that workload forecasts are prepared to identify trends and to provide information needed for the capacity plan.

3.7 Capacity Management of Resources

Information services function management should establish a planning process for the review of hardware performance and capacity to ensure that cost-justifiable capacity always exists to process the agreed workloads and to provide the required performance quality and quantity prescribed in service level agreements. The capacity plan should cover multiple scenarios.

3.8 Resources Availability

Management should prevent resources from being unavailable by implementing fault tolerance mechanisms, prioritizing tasks and equitable resource allocation mechanisms.

3.9 Resources Schedule

Management should ensure the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.

DS 4.0 - Ensure Continuous Service

4.1 Information Technology Continuity Framework

Information services function management is to create a continuity framework which defines the roles, responsibilities, the risk based approach/methodology to be adopted, and the rules and structures to document the plan as well as the approval procedures.

4.2 Information Technology Continuity Plan Strategy and Philosophy

Management should ensure that the information technology continuity plan is in line with the overall business continuity plan to ensure consistency. Furthermore, the information technology continuity plan should take account of the information technology long- and medium-range plans to ensure consistency.

4.3 Information Technology Continuity Plan Contents

Information services function management should ensure that a written plan is developed containing the following:

* Guidelines on how to use the continuity plan;
* Emergency procedures to ensure the safety of all affected staff members;
* Response procedures meant to bring the business back to the state it was in before the incident or disaster;
* Recovery procedures meant to bring the business back to the state it was in before the incident or disaster;
* Procedures to safeguard and reconstruct the home site;
* Co-ordination procedures with public authorities;
* Communication procedures with stakeholders: employees, key customers, critical suppliers, stockholders and management; and
* Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media.

4.4 Minimizing Information Technology Continuity Requirements

Information services function management should establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.

4.5 Maintaining the Information Technology Continuity Plan

Information services function management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.

4.6 Testing the Information Technology Continuity Plan

To have an effective continuity plan, management needs to assess its adequacy on a regular basis; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.

4.7 Information Technology Continuity Plan Training

The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.

4.8 Information Technology Continuity Plan Distribution

Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorized personnel and should be safeguarded against unauthorized disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.

4.9 User Department Alternative Processing Back-up Procedures

The continuity methodology should ensure that the user departments establish alternative processing procedures that may be used until the information services function is able to fully restore its services after a disaster or event.

4.10 Critical Information Technology Resources

The continuity plan should identify the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs.

4.11 Back-up Site and Hardware

Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these type of services should be concluded.

4.12 Wrap-up Procedures

On successful resumption of the information services function after a disaster, information services function management should establish procedures for assessing the adequacy of the plan and update the plan accordingly.

DS 5.0 - Ensure Systems Security

5.1 Manage Security Measures

Information Technology security should be managed such that security measures are in line with business requirements. This includes:

* translating risk assessment information to information technology security plans;
* implementing the information technology security plan;
* updating the information technology security plan to reflect changes in the information technology configuration;
* assessing the impact of change requests on information technology security;
* monitoring the implementation of the information technology security plan; and
* aligning information technology security procedures to other policies and procedures.

5.2 Identification, Authentication and Access

The logical access to and use of the information services function's computing resources should be restricted by the implementation of an adequate authentication mechanism of identified users and resources associated with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

5.3 Security of Online Access to Data

In an online information technology environment, information services function's management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

5.4 User Account Management

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included.

5.5 Management Review of User Accounts

Management should have a control process in place to review and confirm access rights periodically.

5.6 User Control of User Accounts

Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

5.7 Security Surveillance

The information services function's security administration should ensure that security activity is logged and any indication of imminent security violation is notified immediately to the administrator and is acted upon automatically.

5.8 Data Classification

Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated.

5.9 Central Identification and Access Rights Management

Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

5.10 Violation and Security Activity Reports

The information services function's security administration should assure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.

5.11 Incident Handling

Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

5.12 Re-Accreditation

Management should ensure that re-accreditation of security (e.g., through "tiger teams") is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.

5.13 Counterparty Trust

Organizational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

5.14 Transaction Authorization

Organizational policy should ensure that where appropriate, controls are implemented to provide authenticity of transactions. This requires use of cryptographic techniques for signing and verifying transactions.

5.15 Non-Repudiation

Organizational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third-parties.

5.16 Trusted Path

Organizational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.

5.17 Protection of Security Functions

All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security design, but should not base their security on the design being secret.

5.18 Cryptographic Key Management

Management should define and implement procedures and protocols to be used for generation, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure. If a key is compromised, management should ensure this information is propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms.

5.19 Malicious Software Prevention, Detection and Correction

Regarding malicious software, such as computer viruses or trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures.

5.20 Firewall Architectures and Connections with Public Networks

If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

5.21 Protection of Electronic Value

Management should protect the continued integrity of all cards or similar physical appliances used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

DS 6.0 - Identify and Attribute Costs

6.1 Chargeable Items

Information services function management should ensure that chargeable items are identifiable, measurable and predictable by users. Users should be able to control the use of information services and associated billing levels.

6.2 Costing Procedures

Information services function management should define and implement costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are to be adequately analyzed and reported on to facilitate the cost monitoring. In addition, senior management should periodically evaluate the results of the information service function's job cost accounting procedures, in light of the organization’s other financial measurement systems.

6.3 User Billing and Chargeback Procedures

Information services function management should define and use billing and chargeback procedures. It should maintain user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs. The rate charged should reflect the associated costs of providing services.

DS 7.0 - Educate and Train Users

7.1 Identification of Training Needs

In line with the long-range plan, management should establish and maintain procedures for identifying and documenting the training needs of all personnel using information services. A training curriculum for each group of employees should be established.

7.2 Training Organization

Based on the identified needs, management should define the target groups, identify and appoint trainers, and organize timely training sessions. Training alternatives should also be investigated (internal or external location, in-house trainers or third-party trainers, etc.)

7.3 Security Principles and Awareness Training

All personnel should be trained and educated in system security principles. Senior management should provide an education and training program that includes: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

DS 8.0 - Assist and Advise Information Technology Customers

8.1 Help Desk

User support should be established within a "help desk" function. Individuals responsible for performing this function should closely interact with problem management personnel.

8.2 Registration of Customer Queries

Procedures should be in place to ensure that all customer queries are adequately registered by the help desk.

8.3 Customer Query Escalation

Help desk procedures should ensure that customer queries which cannot immediately be resolved are appropriately escalated within the information services function.

8.4 Monitoring of Clearance

Management should establish procedures for timely monitoring of the clearance of customer queries. Long outstanding queries should be investigated and acted upon.

8.5 Trend Analysis and Reporting

Procedures should be in place which assure adequate reporting with regard to customer queries and resolution, response times and trend identification. The reports should be adequately analyzed and acted upon.

DS 9.0 - Manage the Configuration

9.1 Configuration Recording

Procedures should be in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition. These procedures should also provide for the authorized disposal and consequential sale of configuration items. Moreover, procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of changed records.

9.2 Configuration Baseline

Information services function management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes.

9.3 Status Accounting

Information services function management should ensure that the configuration records reflect the actual status of all configuration items including the history of changes.

9.4 Configuration Control

Procedures should ensure that the existence and consistency of recording of the information services function configuration is periodically checked.

9.5 Unauthorized Software

Information services function management should periodically check the organization's personal computers for unauthorized software.

9.6 Software Storage

A file storage area (library) should be defined for all valid software items in appropriate phases of the system development life cycle. These areas should be separated from each other and from development, testing and production file storage areas.

DS 10.0 - Manage Problems and Incidents

10.1 Problem Management System

Information services function management should define and implement a problem management system to ensure that all operational events which are not part of the standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. Incident reports should be established in the case of significant problems.

10.2 Problem Escalation

Management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the information technology continuity plan.

10.3 Problem Tracking and Audit Trail

The problem management system should provide for adequate audit trail facilities which allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should closely interwork with change management, availability management and configuration management.

DS 11.0 - Manage Data

11.1 Data Preparation Procedures

Management should establish data preparation procedures to be followed by user departments. In this context, input form design should help to assure that errors and omissions are minimized. Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.

11.2 Source Document Authorization Procedures

Management should ensure that source documents are properly prepared by authorized personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.

11.3 Source Document Data Collection

The organization's procedures should ensure that all authorized source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.

11.4 Source Document Error Handling

Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and
corrected.

11.5 Source Document Retention

Procedures should be in place to ensure original source documents are retained or are reproducible by the organization for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.

11.6 Data Input Authorization Procedures

The organization should establish appropriate procedures to ensure that data input is performed only by authorized staff.

11.7 Accuracy, Completeness and Authorization Checks

Transaction data entered for processing (people-generated, system-generated or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible.

11.8 Data Input Error Handling

The organization should establish procedures for the correction and resubmission of data which was erroneously input.

11.9 Data Processing Integrity

The organization should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.

11.10 Data Processing Validation and Editing

The organization should establish procedures to ensure that data processing validation, authentication and editing is performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.

11.11 Data Processing Error Handling

The organization should establish data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.

11.12 Output Handling and Retention

The organization should establish procedures for the handling and retention of output from its information technology application programs. In case negotiable instruments (e.g., value cards) are the output recipients, special care should be taken to prevent misuse.

11.13 Output Distribution

The organization should establish and communicate written procedures for the distribution of information technology output.

11.14 Output Balancing and Reconciliation

The organization should establish procedures for assuring that output routinely is balanced to the relevant control totals. Audit trails should be provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.

11.15 Output Review and Error Handling

The organization's management should establish procedures for assuring that the accuracy of output reports is reviewed by the provider and the relevant users. Procedures should also be in place for controlling errors contained in the output.

11.16 Security Provision for Output Reports

The organization should establish procedures for assuring that the security of output reports is maintained for those awaiting distribution, as well as those already distributed to users.

11.17 Protection of Sensitive Information During Transmission and Transport

Management should ensure that adequate protection of sensitive information is provided during transmission and transport against unauthorized access, modification and misaddressing.

11.18 Protection of Disposed Sensitive Information

Management should define and implement procedures to ensure the non-disclosure of disposed sensitive organization information. Such procedures should guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third-party.

11.19 Storage Management

Procedures should be developed for data storage which consider retrieval requirements, and cost effectiveness and security policy.

11.20 Retention Periods and Storage Terms

Retention periods and storage terms should be defined for documents, data, programs and reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication.

11.21 Media Library Management System

The information services function should establish procedures to assure that contents of its media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion and that measures are taken to maintain the integrity of magnetic media stored in the library.

11.22 Media Library Management Responsibilities

Housekeeping procedures designed to protect media library contents should be established by information services function management. Standards should be defined for the external identification of magnetic media and the control of their physical movement and storage to support accountability. Responsibilities for media (magnetic tape, cartridge, disks and diskettes) library management should be assigned to specific members of the information services function.

11.23 Back-up and Restoration

Management should implement a proper strategy for back-up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements.

11.24 Back-up Jobs

Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.

11.25 Back-up Storage

Back-up procedures for information technology-related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.

11.26 Archiving

Management should implement a policy and procedures for ensuring that archival meets legal and business requirements, and is properly safeguarded and accounted for.

11.27 Protection of Sensitive Messages

Regarding data transmission over the Internet or any other public network, management should define and implement procedures and protocols to be used to ensure integrity, confidentiality and non-repudiation of sensitive messages.

11.28 Authentication and Integrity

The authentication and integrity of information originated outside the organization, whether received by telephone, voicemail, paper document, fax or e-mail, should be appropriately checked before potentially critical action is taken.

11.29 Electronic Transaction Integrity

Taking into consideration that the traditional boundaries of time and geography are less reliant, management should define and implement appropriate procedures and practices for sensitive and critical electronic transactions ensuring integrity and authenticity of:

- atomicity (indivisible unit of work, all of its actions succeed or they all fail);

* consistency (if the transaction cannot achieve a stable end state, it must return the system to its initial state);

* isolation (a transaction's behavior is not affected by other transactions that execute concurrently); and

* durability (transaction's effects are permanent after it commits, its changes should survive system failures).

11.30 Continued Integrity of Stored Data

Management should ensure that the integrity and correctness of the data kept on files and other media (e.g., electronic cards) is checked periodically. Specific attention should be paid to value tokens, reference files and files containing privacy information.

DS 12.0 - Manage Facilities

12.1 Physical Security

Appropriate physical security and access control measures should be established for information technology facilities, including off-site use of information devices in conformance with the general security policy. Access should be restricted to individuals who have been authorized to gain such access.

12.2 Low Profile of the Information Technology Site

Information services function management should ensure a low profile is kept and the physical identification of the site of its information technology operations is limited.

12.3 Visitor Escort

Appropriate procedures are to be in place ensuring that individuals who are not members of the information services function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.

12.4 Personnel Health and Safety

Health and safety practices should be put in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations.

12.5 Protection Against Environmental Factors

Information services function management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment should be installed.

12.6 Uninterruptable Power Supply

Management should assess regularly the need for uninterruptable power supply batteries and generators for critical information technology applications to secure against power failures and fluctuations. When justified, the most appropriate equipment should be installed.

DS 13.0 - Manage Operations

13.1 Processing Operations Procedures and Instructions Manual

The information services function should establish and document standard procedures for information technology operations (including network operations). All information technology solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.

13.2 Start-up Process and Other Operations Documentation

Information services function management should ensure that the operations staff is adequately familiar and confident with the start-up process and other operations tasks by having them documented, periodically tested and adjusted when required.

13.3 Job Scheduling

Information services function management should ensure that the continuous scheduling of jobs, processes and tasks organized into the most efficient sequence, maximizing throughput and utilization, to meet the objectives set in service level agreements. The initial schedules as well as changes to these schedules should be appropriately authorized.

13.4 Departures from Standard Job Schedules

Procedures should be in place to identify, investigate and approve departures from standard job schedules.

13.5 Processing Continuity

Procedures should require processing continuity during operator shift changes by providing for formal handover of activity, status updates and reports on current responsibilities.

13.6 Operations Logs

Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, timely review and examination of the time sequences of processing and other activities surrounding or supporting processing.

13.7 Remote Operations

For remote operations, specific procedures should ensure that the connection and disconnection of the links to the remote site(s) are defined and implemented.

Monitoring (M)

M 1.0 - Monitor the Processes

1.1 Collecting Monitoring Data

For the information technology and internal control processes, management should ensure relevant performance indicators (e.g., benchmarks) from both internal and external sources, are being defined, and that data is being collected for the creation of management information reports and exception reports regarding these indicators.

1.2 Assessing Performance

Services to be delivered by the information services function should be measured (key performance indicators and/or critical success factors) by management and be compared with target levels. Assessments should be performed of the information services function on a continuous basis.

1.3 Assessing Customer Satisfaction

At regular intervals management should measure customer satisfaction regarding the services delivered by the information services function to identify shortfalls in service levels and establish improvement objectives.

1.4 Management Reporting

Management reports should be provided for senior management's review of the organization's progress toward identified goals. Upon review, appropriate management action should be initiated and controlled.

M 2.0 - Assess Internal Control Adequacy

2.1 Internal Control Monitoring

Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations should evoke analysis and corrective action.

2.2 Timely Operation of Internal Controls

Reliance on internal controls requires that controls operate promptly to highlight errors and inconsistencies, and that these are corrected before they impact production and delivery. Information regarding errors, inconsistencies and exceptions should be kept and systematically reported to management.

2.3 Internal Control Level Reporting

Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system. Actions should be taken to identify what information is needed at a particular level of decision making.

2.4 Operational Security and Internal Control Assurance

Operational security and internal control assurance should be established with self-assessment or independent audit to examine whether or not the security and internal controls are operating according to the stated or implied security and internal control requirements. Ongoing monitoring activities by management should look for vulnerabilities and security problems.

M 3.0 - Obtain Independent Assurance

3.1 Independent Security and Internal Control Certification/Accreditation of Information Technology Services

Management should obtain independent certification/accreditation of security and internal controls prior to implementing critical new information technology services and re-certification/re-accreditation of these services on a routine cycle after implementation.

3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers

Management should obtain independent certification/accreditation of security and internal controls prior to using information technology service providers and re-certification/re-accreditation on a routine cycle.

3.3 Independent Effectiveness Evaluation of Information Technology Services

Management should obtain independent evaluation of the effectiveness of information technology services on a routine cycle.

3.4 Independent Effectiveness Evaluation of Third-Party Service Providers

Management should obtain independent evaluation of the effectiveness of information technology service providers on a routine cycle.

3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments

Management should obtain independent assurance of the information service function's compliance with legal and regulatory requirements, and contractual commitments on a routine cycle.

3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers

Management should obtain independent assurance of third-party service providers' compliance with legal and regulatory requirements and contractual commitments on a routine cycle.

3.7 Competence of Independent Assurance Function

Management should ensure that the independent assurance function possesses the technical competence, and skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner.

3.8 Proactive Audit Involvement

Information Technology management should seek audit involvement in a proactive manner before finalizing information technology service solutions.

M 4.0 - Provide for Independent Audit

4.1 Audit Charter

A charter for the audit function should be established by the organization’s senior management. This document should outline the responsibility, authority and accountability of the audit function. The charter should be reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.

4.2 Independence

The auditor should be independent from the auditee in attitude and appearance (actual and perceived). Auditors should not be affiliated with the section or department being audited, and, to the extent possible, should also be independent of the subject organization itself. Thus, the audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

4.3 Professional Ethics and Standards

The audit function should ensure adherence to applicable codes of professional ethics (e.g., Code of Professional Ethics of the Information Systems Audit and Control Association) and auditing standards (e.g., Standards for Information Systems Auditing of the Information Systems Audit and Control Association) in all that they do. Due professional care should be exercised in all aspects of the audit work, including the observance of applicable audit and information technology standards.

4.4 Competence

Management should ensure that the auditors responsible for the review of the organization's information services function activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to information systems auditing tasks maintain their technical competence through appropriate continuing professional education.

4.5 Planning

Senior management should establish a plan to ensure that regular and independent audits are obtained regarding the effectiveness, efficiency and economy of security and internal control procedures, and management's ability to control information services function activities. Senior management should determine priorities with regard to obtaining independent audits within this plan. Auditors should plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards.

4.6 Performance of Audit Work

Audits should be appropriately supervised to provide assurances that audit objectives are achieved and applicable professional auditing standards are met. Auditors should ensure that they obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

4.7 Reporting

The organization's audit function should provide a report, in an appropriate form, to intended recipients upon the completion of audit work. The audit report should state the scope and objectives of the audit, the period of coverage, and the nature and extent of the audit work performed. The report should identify the organization, the intended recipients and any restrictions on circulation. The audit report should also state the findings, conclusions and recommendations concerning the audit work performed, and any reservations or qualifications that the auditor has with respect to the audit.

4.8 Follow-up Activities

Resolution of audit comments rests with management. Auditors should request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

Appendix I - CobiT Project Description

Organization & Responsibilities

The project continues to be supervised by a Project Steering Committee formed by international representatives from industry, academia, government and the audit profession. Overall project guidance is provided by the Executive Board of ISACF. The Project Steering Committee has been instrumental in the development of the CobiT Framework and in the application of the research results.

International working groups were established for the purpose of quality assurance and expert review of the project's interim research and development deliverables.

Research

Research included collection and analysis of identified sources and was carried out by research teams in Europe (Free University of Amsterdam), the USA (California Polytechnic University) and Australia (University of New South Wales). Research teams were staffed with academic and professional representatives.

After collection and analysis, the researchers were challenged to examine each domain and process in depth and suggest new control objectives applicable to that particular information technology process. The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing, industry practices and requirements and industry-specific requirements, as they relate to the framework and to individual control objectives. Their efforts have produced more than 300 new and updated control objectives for consideration by the quality reviewers and the expert groups.

Consolidation of the results was primarily performed by the Project Team, composed of the Project Director, the Project Manager and the Director of Research of ISACF.

Approach and Source Material

Following the development of the framework by the Steering Committee, challenged and updated by the Expert Groups, individual comparison of Control Objectives with each of the identified documents and standards was performed by the research groups.

The intention was not to perform a global analysis of all material nor a redevelopment of Control Objectives from scratch. It was more a comparison and update process.

The basic deliverable from this research activity was a list of primary matches (in the Control Objectives but not in the comparison material), and secondary matches (in the comparison material but not in the Control Objectives).